



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,898	04/27/2001	Erlend Olson	41705/SAH/B600	1523

23363 7590 06/03/2005

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER

SON, LINH L D

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/844,898

Applicant(s)

OLSON ET AL.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 April 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-47 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-47 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is responding to the amendment received on 02/08/05
2. Claim 42 is amended. Claim 47 is newly added.
3. Claims 1-47 are pending.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4-8, 10-22, 24-38, 40-41, and 43-47 are rejected under 35 U.S.C. 102(e) as being anticipated by Etzel et al, US Patent No. 6577734B1, hereinafter "Etzel".

5. As per claims 1 and 7, "A system for distributing cryptographic keys for encrypting digital data, the system comprising: a first memory for storing a cryptographic key" is taught by Etzel in (Fig 1, and Col 3 lines 50-60); "a digital data input medium for receiving digital data to be encrypted; a second memory" is taught by Etzel in (Fig 5, 10, and Col 2 lines 51-60); and a selector (Fig 5, and Col 9 lines 10-15) for coupling the first memory to the second memory via the digital data input medium, wherein the second memory is used to store the cryptographic key temporarily before the cryptographic key

Art Unit: 2135

is used for encrypting the digital data” is taught by Etzel in (Fig 1, 25, and Col 2 lines 51-60, and lines 40-50).

6. As per claims 2, 8, 22, 38, and 40, “the system for encrypting digital data according to claims 1, 7, 12, 22, 38, and 44, wherein the digital data comprises digital video data” is taught by Etzel in (Col 2 lines 45-48).

7. As per claims 4, 10, 24, and 45, the system for encrypting digital data according to claims 1, 8, 12, and 30, wherein the digital data comprises multimedia data” is taught by Etzel in (Col 2 lines 35-40).

8. As per claims 5, 11, 25, and 41, “The system according to claims 1, 7, 12, and 30, wherein the digital data is encrypted in accordance with the High-bandwidth Digital Content Protection specification” is taught by Etzel in (Col 1 lines 30-40).

9. As per claims 6 and 26, “the system for encrypting digital data according to claims 1 and 12, wherein the first input terminal, the second input terminal, the encryptor and the first output terminal are implemented on a single integrated circuit (IC) chip” is taught by Etzel in (Col 2 lines 51-60, and Fig 1, 25).

10. As per claims 12, 16, 30, and 32, “A system for encrypting digital data, the system comprising: a first input terminal for receiving the digital data” is taught by Etzel

Art Unit: 2135

in (Figure 5, 16, Col 4 lines 14-20); "a second input terminal for receiving a key" is taught by Etzel in (Figure 1, 30, Col 2 lines 53-60); "an encryptor for receiving and encrypting the digital data using the key" is taught by Etzel in (Col 2 lines 53-60); and "a first output terminal for transmitting the encrypted digital data, wherein the system receives the key from an external key storage unit via the second input terminal during operation of the system" is taught by Etzel in (Col 2 lines 53-60, and Col 3 lines 7-15).

11. As per claims 13 and 31, "the system for encrypting digital data according to claims 12 and 30, the system further comprising random access memory (RAM) for storing the key before the key provided to the encryptor to be used for encryption of the digital data" is taught by Etzel in (Col 9 line 3).

12. As per claim 14, "the system for encrypting digital data according to claim 13, the system further comprising a multiplexer coupled to the first input terminal and the second input terminal, wherein the multiplexer outputs either the digital data from the first input terminal or the key from the second input terminal" is taught by Etzel in (Col 10 lines 1-5).

13. As per claim 15, the system for encrypting digital data according to claim 14, the system further comprising a selector switch for receiving the digital data and the key from the multiplexer, wherein the selector switch provides the digital data to the

Art Unit: 2135

encryptor, and wherein the selector switch provides the key to the RAM” is taught by Etzel in (Col 9 line 15-29 and lines 40-50, and Col 10 lines 1-8).

14. As per claims 17 and 33, “the system for encrypting digital data according to claims 12 and 30, wherein the second input terminal receives the key as a plurality of key segments” is taught by Etzel in (Col 9 lines 37-39).

15. As per claims 18-19 and 34-35, “the system for encrypting digital data according to claims 12, 18 and 34, wherein the first output terminal is used to transmit the decryption key” is taught by Etzel in (Col 5 lines 60-63, and Fig 1, 41).

16. As per claim 20, Etzel discloses “The system for encrypting digital data according to claim 19, wherein the decryption key is encoded prior to being transmitted via the first output terminal” in (Col 6 lines 30-45).

17. As per claim 27, “the system for encrypting digital data according to claim 12, wherein the second input terminal comprises a control bus, and wherein the system further comprises a controller coupled to the control bus, wherein the controller controls data flow in the system” is taught by Etzel in (Col 9 lines 10-15, and Fig 5).

18. As per claim 28, “the system of encrypting digital data according to claim 27, wherein the control bus comprises an I²C bus” is taught by Etzel in (Col 9 line 60).

19. As per claim 29, "the system of encrypting digital data according to claim 27, wherein the controller is selected from a group consisting of a finite state machine (FSM), a microprocessor and a micro controller" is taught by Etzel in (Col 9 lines 10-15).

20. As per claim 43, "the system according to claim 42, wherein the digital data transmitter comprises a Digital Versatile Disk (DVD) player" is taught by Etzel in (Col 2 lines 40-43).

21. As per claims 21, 36-37, and 46, "the system according to claims 20, 35-36, and 42, wherein the second encryption key comprises a public key and the second decryption key comprises a private key" is taught by Etzel in (Col 4 lines 35-38).

22. As per claim 47, Etzel discloses "A system for encrypting digital data, the system comprising: a first input terminal for receiving the digital data" in (Fig 1, path 16, Col 2 lines 5-60); "a encryptor for receiving and encrypting the digital data using a key" in (Fig 1, #30, Col 3 lines 50-60), "the encryptor having a key storage provided as an integral component thereon for storing the key" in (Figure 5 #8, Col 9 lines 35-40); and "a first output terminal for transmitting the encrypted digital data" in (Col 9 lines 5-10), "wherein the key storage of the encryptor (security module 30) receives the key from an external key storage medium via the second input terminal during operation of the system" in (Col 3 lines 50-55, memory 26).

Claim Rejections - 35 USC § 103

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

24. **Claims 3, 9, 23, 39, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Etzel.**

25. As per claims 3, 9, 23, and 39, the system for encrypting digital data according to claims 2, 8, 22, and 38. However, "wherein the digital video data is in composite RGB format" is not directly taught by Etzel. Nevertheless, Etzel discloses the digitized video signal and MPEG-2 encoding provided to the user over the cable-TV systems and direct broadcast satellite video systems (Col 1 lines 15-18, and Col 2 lines 45-50). Therefore, it would have been obvious at the time of the invention for one having ordinary skill in the art to recognize that the video broadcasting technology, which is implemented in Etzel's invention, must be RGB (Color) to be compatible with the customer TV display. Further, Black and White movies and images are not favored to the customers.

26. *(New Rejection based on Amendment)* As per claim 42, Etzel discloses "A system for distributing cryptographic keys from a digital data transmitter to a digital data receiver via a digital link" in (Fig 1 #41, Col 7 lines 1-5), "the system comprising: a digital data transmitter comprising a first key storage medium for storing a first encryption key,

Art Unit: 2135

a second encryption key and a first decryption key" in (Fig 1, 40 and 5 #13, Col 3 lines 50-60, and Col 5 lines 55-67, Col 6 lines 25-44); "a data encryptor for using the first encryption key to encrypt digital data, and for using the second encryption key to encrypt the first decryption key; and a data link transmitter system for transmitting the encrypted digital data and the encrypted first decryption key over the digital link" in (Fig 1 #41 and 40, and Col 5 line 50 to Col 6 line 45); and "a digital data receiver comprising: a data link receiver for receiving the encrypted digital data and the encrypted first decryption key over the digital link; a second key storage medium for storing a second decryption key; a data decryptor for using the second decryptor key to decrypt the encrypted first decryption key, and for using the first decryption key to decrypt the encrypted digital data; and a third key storage medium for storing the first decryption key" in (Col 6 lines 44-47, Col 7 lines 23-45 and Fig 5). However, Etzel is silent on the first decryption key is different than the first encryption key. Nevertheless, Etzel does teach a method of encrypting the data and decrypting it using a symmetrical key (Col 6 lines 23-35). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Etzel's invention to implement Asymmetrical key instead to provide additional security to the key and the video program.

Response to Arguments

27. Applicant's arguments filed 02/08/05 have been fully considered but they are not persuasive.

28. As per remark on page 12-13, applicant argues that the "a selector for coupling the first memory to the second memory via the digital data input medium" limitation is not disclosed in Etzel's invention. Applicant has misinterpreted the invention. As cited in column 9 lines 10-15, the selector is the processor 2 in figure 5 or processor 25 in figure 1. As cited in column 3 lines 50-55, the 1st memory is at the process 25 where it is storing the cryptographic key. As cited in Col 2 lines 51-60, the second memory is at the security module 30 where the program gets encrypted. The processor 25 selects the key from its memory 26 and the encoded program via the digital data input medium path 16 and passes or couples both key in the first memory and encoded program to the security module, where the second memory resides (Figure 5, 10, Col 9 lines 1-7), for encrypting as cited in Column 2 lines 51-56 and further elaborated in Col 3 lines 50-60. Therefore, Etzel fully discloses claim 1 and 7.

29. As remark on page 14 last paragraph to page 16 first paragraph, Applicant argues that the limitations of first input terminal and second input terminal are not disclosed by Etzel. Nevertheless, Etzel does disclose both terminals. As described above, the processor 25 gets the encode program via path 16, the first input terminal, and gets the encrypting key from its memory, the second terminal. Then it passes or

Art Unit: 2135

couples both key and program to the encryptor. According to Figure 5, Encryptor diagram, there is an input path and the output path. Etzel also discloses that the key is from the memory 25, which is external of the encryptor. Therefore, claims 12 and 30 are rejected.

30. Claims 1-41 rejection basis dated 11/03/04 is maintained.

31. Applicant amended claim 42, which necessitated new grounds of rejection. See Rejections above.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

32. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see <http://pzr-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

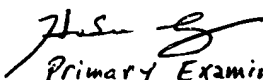
Application/Control Number: 09/844,898

Art Unit: 2135

Linh LD Son

Patent Examiner

Page 12


Primary Examiner
AU 2135